

ABSTRAK

Teknologi pada jaman sekarang banyak dilingkupi oleh kriptografi. Mulai dari percakapan telepon genggam, akses internet, sampai pesan teks telah menggunakan kriptografi. AES-CBC merupakan enkripsi dengan menggunakan kunci dan initial vector, digunakan IV (Initialization Vector) untuk dilakukan XOR dengan blok pertama . Base64 adalah metode pengkodean yang mewakili data biner dalam format string ascii dengan menerjemahkannya kedalam representasi base64. Ada banyak algoritma kriptografi, AES-CBC merupakan enkripsi dengan menggunakan kunci dan initial vector,. Hasil dari penelitian ini adalah algoritma Kriptografi AES-CBC digunakan untuk mengenkripsi pesan dan base64 yang di implementasikan untuk melindungi pesan yang akan di kirim melalui aplikasi chat. Dari penelitian yang dilakukan dapat disimpulkan bahwa hasil berupa 57% pesan yang terdeskripsi memiliki kesamaan dengan isi pesan yang asli karena menggunakan kunci dan initial vector yang sama untuk membuka enkripsi dan, untuk hasil berupa 43% pesan yang terdeskripsi tidak memiliki kesamaan dengan isi pesan yang asli karena menggunakan kunci dan initial vector yang berbeda untuk membuka enkripsi.

Kata kunci: *Kriptografi, aplikasi chatting, AES-CBC, Base64*

ABSTRACT

Current technology is mostly covered by cryptography. Starting from cell phone conversations, internet access, to text messages, they all have used cryptography. Many have applied it to keep messages secret, but now, many tappers already know the techniques to hack it. Therefore, this study attempts to develop an algorithm that is able to keep text messages secret and then tries to implement it into a chat application.

The results of this research show the AES-CBC cryptography algorithm is used to encrypt messages and base64 is implemented to protect messages to be sent via chat applications.

From the research, it can be concluded that the results show that 57% of the messages encrypted have similarities to the contents of the original message, because they use the same key and initial vector to decrypt and, that 43% of the messages that are decrypted have no similarities to the contents of the original message. because they use different key and initial vector to decrypt.

Keywords: cryptography, chatting application, AES-CBC, Base64